Federal Aviation Administration

Current Contract Security Capabilities

Prepared by:

FAA Telecommunications Infrastructure (FTI)-2 Program Office, AJM-3170

Date: October 5, 2015

Table of Contents

1.0 Purpose

This paper provides an overview of the FAA's existing security capabilities in terms of the security services, architecture and the associated challenges as implemented today under the FAA Telecommunications Infrastructure (FTI) contract and documented in the FTI Telecommunications Services Description (FTSD).

2.0 Background

FTI provides a wide range of telecommunications and security services to support operational requirements. FTI services are described in the FTSD and partitioned into service classes having common sets of general performance requirements including Reliability, Maintainability and Availability (RMA) category, latency, call set-up time, call blocking limits, and Service Delivery Point (SDP) to SDP security services. Basic security services for individual telecommunications services are generally an attribute of the telecommunications service class ordered. In some cases additional security features are desired for a particular telecommunication service; these additional security features are ordered as enhanced security service options. The security services for FTI are built to specifications that protect FAA users' information within the FTI Wide Area Network (WAN), i.e., from the SDP in one facility to the SDP in another facility. FTI also provides boundary protection security services that enable communications between FAA programs in different domains and communications from any of the FAA domains with non-FAA partners, such as airlines, providers of weather products, and non-U.S. Air Traffic Control. FTI security services enable a layered security architecture that includes: (1) a basic set of network security services such as authentication, perimeter security, and intrusion detection; and (2) enhanced network security features, such as enhanced access control lists and extranet gateway services, provide additional protection that are available on a service-by-service basis.

The FTI Security Team is responsible for monitoring the heath, status, and configuration of all FTI security management systems and functions. The FTI Security Team has engineered and deployed enhanced monitoring solutions in strategic locations that allow for early detection should an intrusion occur. Dedicated security staff trained in incident detection monitor the network on a 24x7x365 basis and follow strict incident response protocols in the event of an intrusion. The FTI Security Operations Control Center (SOCC) monitors FAA's National Airspace System (NAS) and Administrative traffic for malicious activity utilizing the latest COTS cyber-security technology and FAA-integrated processes and procedures. The FTI SOCC ensures that FTI is hardened and protected from malicious activity.

3.0 Description of Current Environment

The FAA employs a Defense-In-Depth approach to secure the FAA systems in the NAS as well as the environments in which the FAA systems operate. FTI provides the FAA's Wide Area Network (WAN) and also provides the boundary protection to the NAS, the NAS Programs are responsible for the individual Local Area Networks (LANs) at each facility and the components connected to those LANs. Increasingly, FAA systems have the need to communicate with non-

NAS entities, which is facilitated by the FTI NAS Enterprise Security Gateways (NESGs) that are engineered to provide additional layers of security for NAS systems. To further enhance security, communication is limited to only those non-NAS entities that have received approval from the FAA. Multiple layers of separation and controls are implemented between the external environment and the secure NAS environment as shown in Figure 1 below.

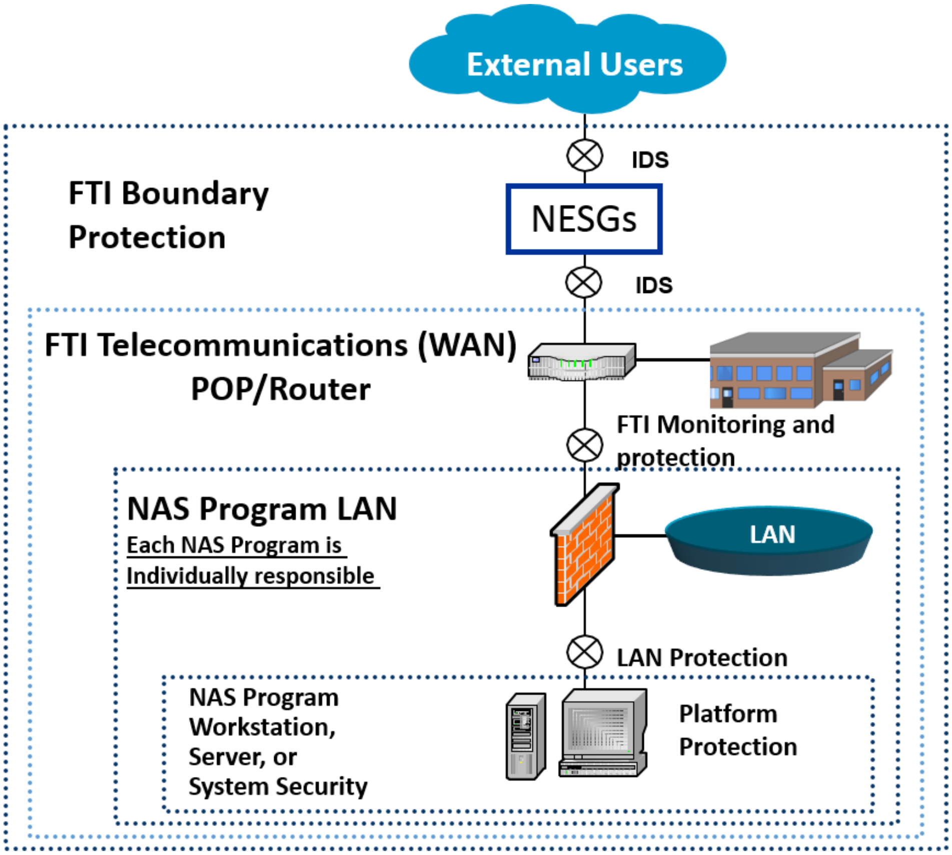
External Users
IDS
FTI Boundary Protection
NESGs
IDS
FTI Telecommunications (WAN) POP/Router
FTI Monitoring and protection
NAS Program LAN
Each NAS Program is Individually responsible
LAN
LAN Protection
NAS Program Workstation, Server, or System Security
Platform Protection

Figure 1: FAA NAS Defense-In-Depth

The NESG architecture is flexible in that it can provide a number of security control combinations to accommodate external users and FAA programs. Ultimately, the gateways provide an important component of a consolidated, centrally managed and secure approach toward enterprise boundary protection. The boundary protection gateways will continue to evolve as NAS systems introduce new technology and standards.

4.0 FAA Critical Challenges

A key challenge is the evolution of the FAA's security approach to address the transition to NextGen. The FAA is adapting to assure system and network security using all methods available from acquisition to design to operations. NextGen systems are being designed using industry standards for both security and operations as well as to integrate with the existing NAS approach to security. Designs for NextGen systems consider all elements of the 'system of systems' with attention paid to each interface to understand vulnerabilities and identify mitigating factors.

The FAA will also need to continually evolve its NAS Operational IP network with state-of-the-art "Boundary Protection" capabilities, which provides secure mechanisms for collaboration with partners in a secure and reliable manner. These networking and boundary protection capabilities are being designed and developed in close collaboration with evolving NAS programs, including FAA Cloud Services; i.e. the evolution of NAS cyber security capabilities are being designed in close coordination with evolving NextGen systems and concepts of operations to ensure these new systems can effectively leverage advancements in infrastructure cyber security.

5.0 Questions

1. As FAA Programs increasingly communicate with non-NAS entities and more information products are added to the NESG infrastructure, user demand will become more dynamic and difficult to predict. What considerations and potential technical solutions could help manage the FAA's Boundary Protection Gateway resources?
2. From a Defense-In-Depth perspective, should NAS boundary protection be offered as an enterprise service by the telecommunications service provider or provided by an independent entity?
3. As the need for additional end-to-end security monitoring increases, how can this be accomplished while avoiding impact on network performance or significant consumption of network management resources?
4. With the potential leverage of Cloud Processing in the NAS, what considerations or technologies could be helpful in developing an efficient and secure infrastructure for support the transition of some FAA functionality to FAA Cloud Services?

   Note: The scope of the existing FTI contract does not include Cloud computing services, but FTI is used to provide secure telecommunications connectivity between the Cloud Service Provider's data centers.